

10-12-06

AF
GFW

Reply Brief
Appl. No.: 09/843,069
Submitted: October 10, 2006



**BEFORE THE BOARD OF PATENT APPEALS AND
INTERFERENCES**

Application Number: 09/843,069
Filing Date: April 26, 2001
Appellants: BURNETT ET AL.

Primary Examiner:
Kristin D. Sandoval

REPLY BRIEF

"Express Mail" Mailing Label

Number EQ 994237590 US

Date of Deposit: October 10, 2006

I hereby certify that this paper or fee is being deposited
with the United States Postal Services "Express Mail
Post Office to Addressee" service under 37 CFR 1.10
on the date indicated above and is addressed to the
Commissioner of Patents and Trademarks,
P. O. Box 1450,
Alexandria, Virginia 22313-1450

Darrell Walker
Darrell Walker, Reg. No. 34,945

This reply brief is in response to the Examiner's Answer filed August 8, 2006 responding to the Appellants' Appeal May 22, 2006.

Background of the present invention

This invention describes a method for file system security through techniques that control access to the file system resources using externally stored attributes. The invention accomplishes the objective in a file system security by creating an external database containing auxiliary attributes for objects in the file system. This solution incorporates techniques and algorithms for attribute attachment, storage and organization of the associations to these attributes, and subsequent recognition of attached attributes. In this approach, the attributes would define authorization policy for controlling access to objects in the file system. Such a solution would require techniques for associating the defined policy with file system objects, detecting accesses to the objects, locating the appropriate attributes at access time, and then processing the attributes to produce an access decision for granting or denying access to the accessed resource.

Background of Kenton (5,479,612)

Kenton describes a system and method of encouraging computer system customers to purchase licenses before employing certain types of peripheral devices for use with their computer system. The computer system establishes contact with a peripheral device. It then verifies that the peripheral device is supported by the operating system. If the peripheral device is supported, the system determines whether the peripheral device is licensed (and therefore requires a driver license key in order for the peripheral device to be accessed by the system). If the peripheral device requires a driver license, the system determines whether the corresponding driver license key is installed in the keys file of the computer system. If the driver license key is not installed, the system compels (or encourages) installation of the driver license key by (1) displaying a licensing violation message instructing the customer to obtain the proper license; and/or (2) precluding access of the peripheral device by the computer system.

Distinction between Inventions

The both relate to device access and discuss searching a database to find entries related to the device. However, that it were the similarities stop. The methods and goals of the items are very different. The patent deals with a computer device driver allowing the computer as a whole to support access to the device as a whole and it relates to the hardware connection relationship between the computer and the device.

The present invention pertains to methods for advanced fine-grained discretionary access controls on filesystem (objects that represent access paths to devices). Those devices may be physical devices or s/w abstractions of devices. In summary, the present invention is fundamentally about access controls on filesystem objects that represent devices, not access means between the computer and the physical device.

From there, the ensuing claims and descriptions in the Applicants' present invention define different methods, when compared to Kenton, for device access control, and the methods are applied and enforced on access attempts through the filesystem object that represents the device.

Response to Arguments in Examiner's Answer

The rejections to claims 1-21 are novelty rejections based on 35 U.S.C. 102(b) citing Kenton et al. (U.S. Patent 5,479,612).

Per claim 1, the Examiner asserts that Kenton discloses each element of the claim. In particular, one assertion is that Kenton discloses the step of: searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device (Fig. 2, steps 19 and 20, p. 3 [0025]). The examiner cites column 4, lines 29-33 and column 5, lines 18-22 to support this assertion.

The distinctions between Kenton and the present invention can be illustrated contrasting Figure 2 of the Applicants' present invention with Figure 2 of Kenton. Referring to Applicants' Figure 2, step 19 describes a mapping step in which searches a mapping database (created in FIG. 1) for all of the special device files in the database that

represent the device that is the object of this access attempt. This step generates a list of device files in the database that refer to the requested system device. Kenton does not generate this list of device files. In Kenton, each peripheral device may have a file, but Kenton does not describe a list of device files for a device. Further, the authorization decision of Applicant's present invention is not disclosed in Kenton. Again referring to Figure 2, steps 22-25 describe the authorization decision process of Applicants' present invention. The decision step cited in Kenton (column 5, lines 36-47) describes a quantity fields summation process. Applicants' present invention describes an entry by entry (of the entries in the generated list) determination. In step 23, for the first file list entry, the decision component of the security manager will determine whether this user or application making the present access attempt would have access to the device through the security rules for the device file path (PON) associated with this file list entry. If the decision is that this access attempt would be granted under the security rules associated with the present file list entry, step 24, then the process determines whether there are more entries in the file entry list, step 25. If there are more entries, the process returns to step 22 and repeats the steps 22 through 25 for the next file list entry. If the determination in step 24 is that there would be no access grant for the present access attempt under the security rules for the current file list entry, the technique would deny the access attempt, step 26 and the process ends. If the present file access attempt would be granted under the security rules of each file list entry, then the authorization decision engine would grant access to the file device even though the particular device file used in the present file access attempt, even though that device file is not protected, step 27. In Applicants' present invention, each device file in the list must be granted access before the access attempt is successful (See claim 8).

Claims 2 and 3 further illustrates distinctions between Kenton and the present invention. These claims cover situations in which the database contains special device files and when the database does not contain a special device file. The present invention is applicable to special device files. If the files found in the database are not special device files, the method terminates. In this case, the method is applicable. The location in Kenton cited by the examiner (column 4, lines 30-40) is for the case when there is not

a match. The step in Kenton, step 204 as cited by the examiner, precludes access. Steps 17 and 18 of the present invention preclude this method from continuing.

In claim 4, the sections of Kenton cited by the Examiner do not describe the claimed elements. Kenton does not describe the specific steps of comparing the file name of a device making an access attempt to the protected object name in the database entry. This section of Kenton discusses the storing of a violation log.

Claim 8 of the present invention describes an authorization decision step that performs a one by one comparison of each entry in the special device file entry list. As mentioned, each entry has to be granted access before the access attempt is granted. Kenton uses valid keys that come from devices in a group from which the access attempt is initiated. If the sum of the valid keys is less than the number of devices currently accessing the system, the access attempt is denied.

Although, this process is an authorization process, it is not the authorization process of the present invention. Further, the mere fact that methods may have some common or similar attributes does not mean that the methods are the same or that one method anticipates the other method.

As previously mentioned, both relate to device access and discuss searching a database to find entries related to the device. However, the Kenton patent deals with a computer device driver allowing the computer as a whole to support access to the device as a whole and it relates to the hardware connection relationship between the computer and the device. The present invention pertains to methods for advanced fine-grained discretionary access controls on filesystem (objects that represent access paths to devices). Those devices may be physical devices or s/w abstractions of devices (Not described in Kenton). The present invention is fundamentally about access controls on filesystem objects that represent devices, not access means between the computer and the physical device.

With regard to claim 20, contrary to the examiner's assertion that Kenton (column 4, lines 41-44) describe an externally stored authorization program overlaying said native operating system and augmenting the standard security controls of said native operating

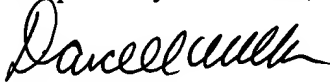
system, the cited location in Kenton (column 4, lines 41-44) do not describe such a system. Therefore the examiner's assertion is not supported by the cited reference.

CONCLUSION

Applicants submit that all of the pending claims are in condition for allowance. Applicants further submit that the amendments as discussed with the Examiner were for the purpose of further defining the impersonator programs of the present invention. Applicants believe that no additional search should be required in view of the type of amendments Applicants made to the claims. Therefore, withdrawal of the rejections and passage to issuance is respectfully requested.

In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

Respectfully Submitted,



Darcell Walker

Reg. No. 34,945

9301 Southwest Freeway, Suite 250

Houston, Texas 77074

713-772-1255

October 10, 2006

APPENDIX I CLAIMS

Claim 1 (Previously presented) A method for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

retrieving file attributes for a device file resource used in the system device access attempt; (Fig. 2, step 16, p. 3 [0025])

determining whether the resource that is making the access attempt is a special device file; (Fig. 2, steps 17 and 18, p.3 [0025])

searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a special device file entry list of all protected device files that represent said system device (Fig. 2, steps 19 and 20, p. 3 [0025]); and

generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list (Fig. 2, steps 22, 23, 24, 25, 26 and 27, p.3 [0025-p. [0026]]).

Claim 2 (Original) The method as described in claim 1 further comprising before said searching step the step of terminating said access control method when the accessing resource is not a special device file.

Claim 3 (Previously presented) The method as described in claim 1 further comprising after said searching step the step of terminating said access control method when said searching step did not find any database entries that had device specifications that match device specifications of the special device file making the access attempt.

Claim 4 (Previously presented) The method as described in claim 1 wherein said searching step comprises the steps of: retrieving an entry from the mapping database; comparing device specifications of the special device file making the access attempt to device specifications of the database entry; and comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 5 (Original) The method as described in claim 4 further comprising after said file name comparison step the steps of: generating a device file entry list containing the database entry with the same file specification and file name as the device file making the access attempt; and terminating said searching step.

Claim 6 (Previously presented) The method as described in claim 4 further comprising after said file name comparison step the steps of placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 7 (Previously presented) The method as described in claim 6 further comprising the steps of:

- determining whether there are more entries in the database;
- retrieving a next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and
- returning to said special device file comparison step.

Claim 8 (Previously presented) The method as described in claim 2 wherein said authorization decision step comprises the steps of:

- retrieving the current entry in the special device file entry list;
- calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;
- determining whether decision component granted access;
- determining whether more entries are in said special device file entry list, if decision component granted access; and
- updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 9 (Previously presented) The method as described in claim 8 further comprising after said decision determination step the step of denying the access attempt to the system device if the decision component of a special device file entry denies access.

Claim 10 (Previously presented) The method as described in claim 8 further comprising the step of allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 11 (Original) A method for controlling access to a computing system device being accessed through a device file, said access control being through an externally stored resource and comprising the steps of:

- monitoring the computing system for activities related to creating and accessing special device files that represent system devices; (p. 2, [0015])
- restricting the creation of special device files based on rules defined in the externally stored resource (p. 4 [0027]); and
- restricting special device file accesses based on rules defined in the externally stored resource (p. 4 [0028], Fig. 5 element 57).

Claim 12 (Previously presented) A computer program product in a computer readable medium for controlling access to a computer system device, being accessed through a special device file, with externally stored resources comprising the steps of:

instructions for retrieving file attributes for a device file resource used in the system device access attempt; (Fig. 2, step 16, p. 3 [0025])

instructions for determining whether the resource that is making the access attempt is a special device file; (Fig. 2, steps 17 and 18, p.3 [0025])

instructions for searching a mapping database for special device files that represent the system device that is the object of the access attempt and generating a device file entry list of all protected device files that represent said system device (Fig. 2, steps 19 and 20, p. 3 [0025]); and

instructions for generating an authorization decision for the access attempt to the system device based on the security policy that governs each device file in the special device file entry list (Fig. 2, steps 22, 23, 24, 25, 26 and 27, p.3 [0025-p. [0026]]).

Claim 13 (Previously presented) The computer program product as described in claim 12 wherein said instructions for searching a mapping database comprise:

instructions for retrieving an entry from the mapping database;

instructions for comparing the device specification of the special device file making the access attempt to the device specification of the database entry; and

instructions for comparing the file name of the special device file making the access attempt to the protected object name of the database entry.

Claim 14 (Previously presented) The computer program product as described in claim 13 further comprising after said file name comparison instructions: instructions for generating a special device file entry list containing the database entry with the same file specification and file name as the special device file making the access attempt; and instructions for terminating said searching instructions.

Claim 15 (Previously presented) The computer program product as described in claim 13 further comprising after said file name comparison instructions the instructions for placing in a file entry list, a mapping database entry having the same file specification as, but different file name from the special device file making the access attempt.

Claim 16 (Previously presented) The computer program product described in claim 15 further comprising:

- instructions for determining whether there are more entries in the database;

- instructions for retrieving the next mapping database entry for comparison with said special device file making the access attempt, when more entries are found in the mapping database; and

- instructions for returning to said special device file comparison step.

Claim 17 (Presently presented) The computer program product as described in claim 12 wherein said authorization instructions comprise:

- instructions for retrieving the current entry in the special device file entry list;

- instructions for calling the access decision component to obtain an access decision for the access attempt to the system device based on the security policy that governs the current entry in the device file entry list;

- instructions for determining whether decision component granted access;

- instructions for determining whether more entries are in said special device file entry list, if decision component granted access; and

- instructions for updating current entry in said special device file entry list and returning to said current entry retrieving step.

Claim 18 (Original) The computer program product as described in claim 17 further comprising after said decision determination instructions the instructions for denying the access attempt to the system device if the decision component denies access.

Claim 19 (Previously presented) The computer program product as described in claim 17 further comprising instructions for allowing the access attempt to the system device if no more entries are in the special device file entry list.

Claim 20 (Original) A computer connectable to a distributed computing system, which includes special device files containing information, related to corresponding system devices comprising:

- a processor; (Fig. 6)
- a native operating system; (Fig. 5)
- application programs; (Fig. 5, element 55)
- an externally stored authorization program overlaying said native operating system and augmenting the standard security controls of said native operating system (p.5 [0030]);
- a mapping database within said external authorization program containing a system device to a protected object name entries for each protected file system object (Fig. 5, elements 56,57 and 58 and p.5 [0030]); and
- a decision component within said authorization program for controlling access to special device files representing system devices (Fig. 5, element 57).

Claim 21 (Original) The computer as described in claimed 20 further comprising authorization program for restricting the creation of special device files representing protected system devices.